

# Release Notes

## FortiManager 7.0.6



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



July 12, 2023

FortiManager 7.0.6 Release Notes

02-706-861341-20230712

# TABLE OF CONTENTS

<b>Change Log</b>	<b>6</b>
<b>FortiManager 7.0.6 Release</b>	<b>7</b>
Supported models	7
FortiManager VM subscription license	7
Management extension applications	7
Supported models for MEA	8
Minimum system requirements	8
<b>Special Notices</b>	<b>10</b>
FortiManager fails to retrieve FortiGate's configuration when external-resource objects include a "g-" prefix	10
FortiManager 7.0.6 GUI issues in Google Chrome and Microsoft Edge	10
FortiManager creates faulty dynamic mapping for VPN manager interface during PP import	11
FAP-831F not yet supported by AP Manager	11
Installing policy packages with 80K rules	11
Authorizing FortiGate with FortiClient EMS connected	11
View Mode is disabled in policies when policy blocks are used	11
FortiManager upgrades from 7.0.0	12
Fortinet verified publisher docker image	12
Scheduling firmware upgrades for managed devices	13
Modifying the interface status with the CLI	13
SD-WAN with upgrade to 7.0	13
Citrix XenServer default limits and upgrade	14
Multi-step firmware upgrades	14
Hyper-V FortiManager-VM running on an AMD CPU	14
SSLv3 on FortiManager-VM64-AWS	14
<b>Upgrade Information</b>	<b>16</b>
Downgrading to previous firmware versions	16
Firmware image checksums	17
FortiManager VM firmware	17
SNMP MIB files	18
<b>Product Integration and Support</b>	<b>19</b>
Supported software	19
Web browsers	20
FortiOS and FortiOS Carrier	20
FortiADC	20
FortiAnalyzer	20
FortiAuthenticator	21
FortiCache	21
FortiClient	21
FortiDDoS	21
FortiDeceptor	21

FortiFirewall and FortiFirewallCarrier .....	21
FortiMail .....	22
FortiProxy .....	22
FortiSandbox .....	22
FortiSOAR .....	22
FortiSwitch ATCA .....	23
FortiTester .....	23
FortiWeb .....	23
Virtualization .....	23
Feature support .....	23
Language support .....	24
Supported models .....	25
FortiGate models .....	26
FortiGate special branch models .....	28
FortiCarrier models .....	32
FortiCarrier special branch models .....	33
FortiADC models .....	35
FortiAnalyzer models .....	35
FortiAuthenticator models .....	36
FortiCache models .....	36
FortiDDoS models .....	36
FortiDeceptor models .....	37
FortiFirewall models .....	37
FortiFirewallCarrier models .....	37
FortiMail models .....	38
FortiProxy models .....	38
FortiSandbox models .....	38
FortiSOAR models .....	39
FortiSwitch ATCA models .....	39
FortiTester models .....	39
FortiWeb models .....	40
<b>Compatibility with FortiOS Versions .....</b>	<b>41</b>
FortiManager 7.0.6 and FortiOS 7.0.11 compatibility issues .....	41
<b>Resolved Issues .....</b>	<b>43</b>
AP Manager .....	43
Device Manager .....	43
Others .....	43
Policy and Objects .....	44
System Settings .....	44
VPN Manager .....	44
Common Vulnerabilities and Exposures .....	45
<b>Known Issues .....</b>	<b>46</b>
AP Manager .....	46
Device Manager .....	46
FortiSwitch Manager .....	47
Global ADOM .....	48

---

Others .....	48
Policy & Objects .....	49
Revision History .....	51
System Settings .....	52
VPN Manager .....	52
<b>Appendix A - FortiGuard Distribution Servers (FDS) .....</b>	<b>53</b>
FortiGuard Center update support .....	53
<b>Appendix B - Default and maximum number of ADOMs supported .....</b>	<b>54</b>
Hardware models .....	54
Virtual Machines .....	54

# Change Log

Date	Change Description
2023-03-01	Initial release.
2023-03-02	Updated <a href="#">Special Notices on page 10</a> .
2023-03-08	Updated <a href="#">FortiProxy on page 22</a> and <a href="#">Known Issues on page 46</a> .
2023-03-13	Updated <a href="#">Known Issues on page 46</a> .
2023-03-13	Updated <a href="#">Known Issues on page 46</a> .
2023-03-17	Updated support for FortiGate-601F in <a href="#">FortiGate special branch models on page 28</a> .
2023-03-20	Updated <a href="#">Known Issues on page 46</a>
2023-03-27	Added <a href="#">FortiManager 7.0.6 and FortiOS 7.0.11 compatibility issues on page 41</a> . Updated <a href="#">FortiGate special branch models on page 28</a> .
2023-04-14	Updated <a href="#">FortiOS and FortiOS Carrier on page 20</a> .
2023-04-17	Updated <a href="#">Resolved Issues on page 43</a> .
2023-04-28	Updated <a href="#">FortiManager 7.0.6 and FortiOS 7.0.11 compatibility issues on page 41</a> .
2023-05-02	Updated <a href="#">FortiSandbox on page 22</a> .
2023-06-01	Updated <a href="#">Special Notices on page 10</a> and <a href="#">Web browsers on page 20</a> .
2023-06-05	Updated <ul style="list-style-type: none"><li>• <a href="#">Special Notices on page 10</a></li><li>• <a href="#">Web browsers on page 20</a></li><li>• <a href="#">Known Issues on page 46</a></li></ul>
2023-06-08	Updated <a href="#">Special Notices on page 10</a> and <a href="#">Known Issues on page 46</a> .
2023-06-20	Updated <a href="#">Known Issues on page 46</a> .
2023-06-23	Updated <a href="#">Special Notices on page 10</a> and <a href="#">Known Issues on page 46</a> .
2023-07-12	Updated <a href="#">Special Notices on page 10</a> and <a href="#">Known Issues on page 46</a> .

# FortiManager 7.0.6 Release

This document provides information about FortiManager version 7.0.6 build 0372.



The recommended minimum screen resolution for the FortiManager GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

- [Supported models on page 7](#)
- [FortiManager VM subscription license on page 7](#)
- [Management extension applications on page 7](#)

## Supported models

FortiManager version 7.0.6 supports the following models:

<b>FortiManager</b>	FMG-200F, FMG-200G, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, and FMG-3900E.
<b>FortiManager VM</b>	FMG_DOCKER, FMG-VM64, FMG_VM64_ALI, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-IBM, FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

## FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see [FortiManager VM firmware on page 17](#).

See also [Appendix B - Default and maximum number of ADOMs supported on page 54](#).

## Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 7.0.6.



FortiManager uses port TCP/443 or TCP/4443 to connect to the Fortinet registry and download MEAs. Ensure that the port is also open on any upstream FortiGates. For more information about incoming and outgoing ports, see the [FortiManager 7.0 Ports Guide](#).

## Supported models for MEA

You can use any of the following FortiManager models as a host for management extension applications:

<b>FortiManager</b>	FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, and FMG-3900E.
<b>FortiManager VM</b>	FMG_DOCKER, FMG-VM64, FMG_VM64_ALI, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-IBM, FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

## Minimum system requirements

By default FortiManager VMs use the following system resource settings:

- 4 vCPU
- 8 GB RAM
- 500 GB disk space

Starting with FortiManager 7.0.0, RAM and CPU is capped at 50% for MEAs. (Use the `config system docker` command to view the setting.) If FortiManager has 8 CPUs and 16 GB RAM, then only 4 CPUs and 8 GB RAM are available to MEAs by default, and the 4 CPUs and 8 GB RAM are used for all enabled MEAs.

Some management extension applications have minimum system requirements that require you to increase system resources. The following table identifies the minimum requirements for each MEA as well as the recommended system resources to function well in a production environment.

MEA minimum system requirements apply only to the individual MEA and do not take into consideration any system requirements for resource-sensitive FortiManager features or multiple, enabled MEAs. If you are using multiple MEAs, you must increase the system resources to meet the cumulative need of each MEA.

Management Extension Application	Minimum system requirements	Recommended system resources for production*
<b>FortiAIOps</b>	<ul style="list-style-type: none"> <li>• 8 vCPU</li> <li>• 32 GB RAM</li> <li>• 500 GB disk storage</li> </ul>	No change
<b>FortiPortal</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	No change
<b>FortiSigConverter</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	No change
<b>FortiSOAR</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> </ul>	<ul style="list-style-type: none"> <li>• 16 vCPU</li> </ul>



Management Extension Application	Minimum system requirements	Recommended system resources for production*
	<ul style="list-style-type: none"> <li>• 8 GB RAM</li> <li>• 500 GB disk storage</li> </ul>	<ul style="list-style-type: none"> <li>• 64 GB RAM</li> <li>• No change for disk storage</li> </ul>
<b>Policy Analyzer</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	No change
<b>SD-WAN Orchestrator</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 12 GB RAM</li> </ul>
<b>Universal Connector</b>	<ul style="list-style-type: none"> <li>• 1 GHZ vCPU</li> <li>• 2 GB RAM</li> <li>• 1 GB disk storage</li> </ul>	No change
<b>Wireless Manager (FortiWLM)</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	No change

\*The numbers in the *Recommended system resources for production* column are a combination of the default system resource settings for FortiManager plus the minimum system requirements for the MEA.

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.0.6.

## FortiManager fails to retrieve FortiGate's configuration when external-resource objects include a "g-" prefix

**Scenario:** Multi-VDOM is enabled on FGTs version 6.4 and external-resource objects are created globally; these objects are being used in webfilter and firewall policies. After upgrading the FGTs to v7.0, the FGTs automatically add a "g-" prefix to the global external-resource. However, FMG has not supported this prefix yet, so FMG fails to retrieve FGT's configuration to DB.

**Workaround:** There are two workarounds; use the approach that works best for your environment. If it is possible, create a new backup of your FMG and FGT(s) before making any changes.

First workaround approach:

1. Re-create all threat feeds locally in VDOM configuration and update policies and security profiles that reference them to the local threat feed vs. the global feed.
2. Delete the global threat feed objects.

Second workaround approach:

1. Perform policy reinstallation. FMG adds original threat feed objects within the VDOM configuration without the 'g' prefix.
2. FMG reports 'install OK/verify FAIL' at the end of the policy installation.
3. Run scripts to delete the global threat feed objects (objects with the 'g' prefix) from the FGT.
4. Retrieve the FGT configuration from FMG.
5. Perform another policy installation to update the configuration synchronization status between the FGT and FMG. No commands are pushed during this stage according to the install wizard.

## FortiManager 7.0.6 GUI issues in Google Chrome and Microsoft Edge

The FortiManager 7.0.6 GUI may not work properly in Google Chrome version 114 (114.0.5735.91) and Microsoft Edge version 114 (114.0.1823.37).

For information about supported web browsers, see [Web browsers on page 20](#).

## FortiManager creates faulty dynamic mapping for VPN manager interface during PP import

If policy changes are made directly on the FortiGates, the subsequent PP import creates faulty dynamic mappings for VPN manager.

It is strongly recommended to create a fresh backup of the FortiManager's configuration prior to this workaround. Perform the following command to check & repair the FortiManager's configuration database:

```
diagnose cdb check policy-packages <adom>
```

After executing this command, FortiManager will remove the invalid mappings of vpnmgr interfaces.

## FAP-831F not yet supported by AP Manager

The AP Manager module does not yet support the FAP-831F model.

## Installing policy packages with 80K rules

A minimum of 32 GB of memory is required on FortiManager to support the installation of 80K rules to managed FortiGates.

## Authorizing FortiGate with FortiClient EMS connected

Please follow the steps below when managing FortiClient EMS Connector's configuration via FortiManager:

1. Add a FortiGate device to FortiManager.
2. Create FortiClient EMS Connector's configuration on FortiManager.
3. Install the configuration onto the FortiGate device.

If the order of the steps is not followed, FortiClient EMS may not authorize the FortiGate device.

## View Mode is disabled in policies when policy blocks are used

When policy blocks are added to a policy package, the *View Mode* option is no longer available, and policies in the table cannot be arranged by *Interface Pair View*. This occurs because policy blocks typically contain multiple policies using different incoming and outgoing interfaces, however, *View Mode* is still disabled even when policy blocks respect the interface pair.

## FortiManager upgrades from 7.0.0

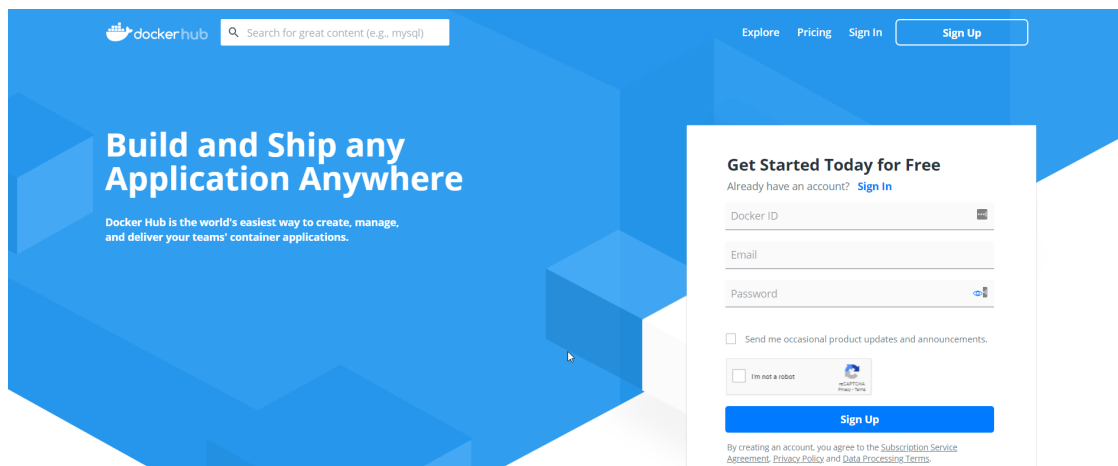
When upgrading from FortiManager 7.0.0, you must first upgrade to 7.0.1 before going to 7.0.2 and later. This is required to correct an issue that causes FortiManager to download unnecessary objects from FortiGuard. Please contact [FortiManager support](#) for more information if required.

## Fortinet verified publisher docker image

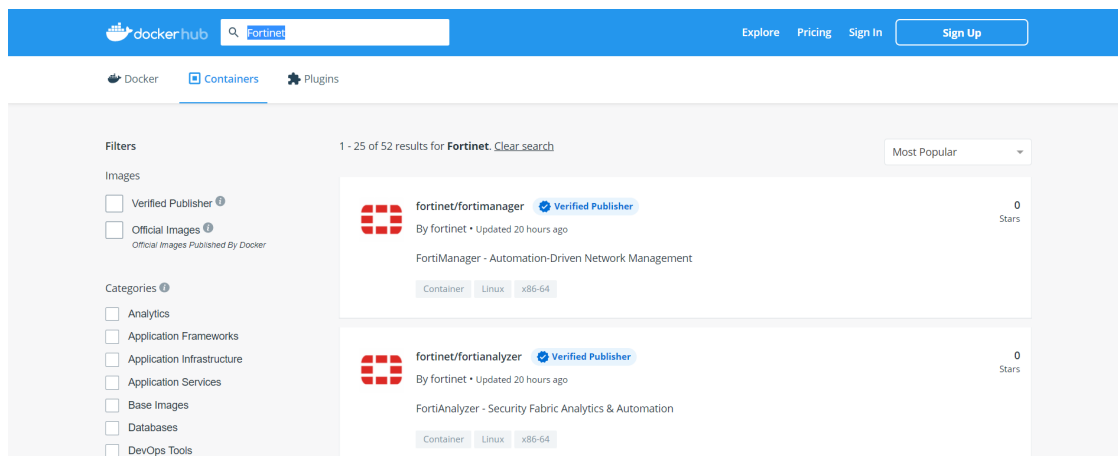
FortiManager docker images are available for download from Fortinet's Verified Publisher public repository on dockerhub.

**To download the FortiManager image from dockerhub:**

1. Go to dockerhub at <https://hub.docker.com/>.  
The dockerhub home page is displayed.

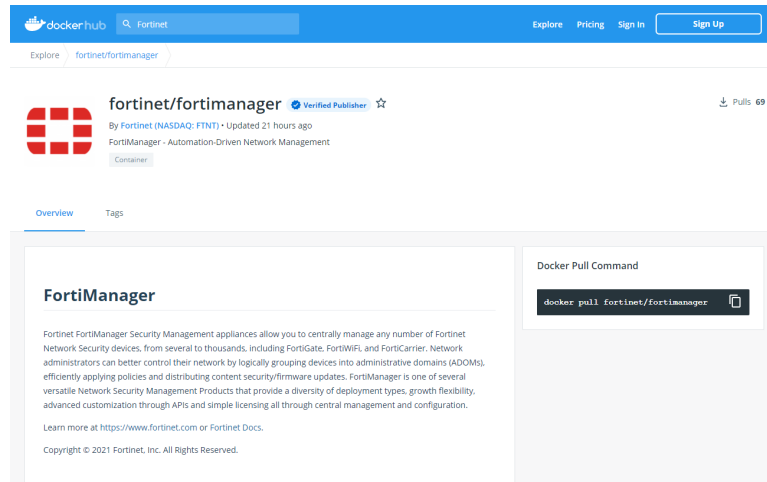


2. In the banner, click *Explore*.
3. In the search box, type *Fortinet*, and press *Enter*.  
The *fortinet/fortimanager* and *fortinet/fortianalyzer* options are displayed.



#### 4. Click *fortinet/fortimanager*.

The *fortinet/fortimanager* page is displayed, and two tabs are available: *Overview* and *Tags*. The *Overview* tab is selected by default.



#### 5. On the *Overview* tab, copy the docker pull command, and use it to download the image.

The CLI command from the *Overview* tab points to the latest available image. Use the *Tags* tab to access different versions when available.

## Scheduling firmware upgrades for managed devices

Starting in FortiManager 7.0.0, firmware templates should be used to schedule firmware upgrades on managed FortiGates. Attempting firmware upgrade from the FortiManager GUI by using legacy methods may ignore the *schedule upgrade* option and result in FortiGates being upgraded immediately.

## Modifying the interface status with the CLI

Starting in version 7.0.1, the CLI to modify the interface status has been changed from *up/down* to *enable/disable*.

For example:

```
config system interface
edit port2
set status <enable/disable>
next
end
```

## SD-WAN with upgrade to 7.0

Due to design change with SD-WAN Template, upgrading to FortiManager 7.0 may be unable to maintain dynamic mappings for all SD-WAN interface members. Please reconfigure all the missing interface mappings after upgrade.

## Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FMG-VM64-XEN image is larger than 128M. Before updating to FortiManager 6.4, increase the size of the ramdisk setting on Citrix XenServer.

### To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:

```
xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
```

2. Confirm the setting is in effect by running `xenstore-ls`.

```
-----  
limits = ""  
pv-kernel-max-size = "33554432"  
pv-ramdisk-max-size = "536,870,912"  
boot-time = ""  
-----
```

3. Remove the pending files left in `/run/xen/pygrub`.



The ramdisk setting returns to the default value after rebooting.

---

## Multi-step firmware upgrades

Prior to using the FortiManager to push a multi-step firmware upgrade, confirm the upgrade path matches the path outlined on our support site. To confirm the path, please run:

```
dia fwmanager show-dev-upgrade-path <device name> <target firmware>
```

Alternatively, you can push one firmware step at a time.

## Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

## SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global  
set ssl-protocol tlsv1
```

end

# Upgrade Information



Prior to upgrading your FortiManager, please review the FortiManager Upgrade Guide in detail as it includes all of the necessary steps and associated details required to upgrade your FortiManager device or VM.

See [FortiManager 7.0.6 Upgrade Guide](#).

You can upgrade to FortiManager 7.0.6 from the following versions:

- FortiManager 6.4.0 to 6.4.x
- FortiManager 7.0.1 to 7.0.x

See also [FortiManager upgrades from 7.0.0 on page 12](#).



Before upgrading FortiManager, check ADOM versions. Check the ADOM versions supported by the destination firmware and the current firmware. If the current firmware uses ADOM versions not supported by the destination firmware, upgrade ADOM versions in FortiManager before upgrading FortiManager to the destination firmware version.

For example, FortiManager 6.4 supports ADOM versions 6.0, 6.2, and 6.4, but FortiManager 7.0 supports ADOM versions 6.2, 6.4, and 7.0. Before you upgrade FortiManager 6.4 to 7.0, ensure that all ADOM 6.0 versions have been upgraded to ADOM version 6.2 or later. See [FortiManager 7.0.6 Upgrade Guide](#).

This section contains the following topics:

- [Downgrading to previous firmware versions on page 16](#)
- [Firmware image checksums on page 17](#)
- [FortiManager VM firmware on page 17](#)
- [SNMP MIB files on page 18](#)

## Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release by using the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrade process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}  
execute format {disk | disk-ext4 | disk-ext3}
```



## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. After logging in, go to *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

## FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

### Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

### Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

### Google Cloud Platform

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.gcp.zip`: Download the 64-bit package for a new FortiManager VM installation.

### Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

### Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `<product>_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.

### Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `<product>_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.



Microsoft Hyper-V 2016 is supported.

---

### Oracle Private Cloud

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.opc.zip`: Download the 64-bit package for a new FortiManager VM installation.

### VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.



For more information see the [FortiManager Data Sheet](#) available on the Fortinet web site. VM installation guides are available in the [Fortinet Document Library](#).

---

## SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

# Product Integration and Support

This section lists FortiManager 7.0.6 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

- [Supported software on page 19](#)
- [Feature support on page 23](#)
- [Language support on page 24](#)
- [Supported models on page 25](#)

## Supported software

FortiManager 7.0.6 supports the following software:

- [Web browsers on page 20](#)
- [FortiOS and FortiOS Carrier on page 20](#)
- [FortiADC on page 20](#)
- [FortiAnalyzer on page 20](#)
- [FortiAuthenticator on page 21](#)
- [FortiCache on page 21](#)
- [FortiClient on page 21](#)
- [FortiDDoS on page 21](#)
- [FortiDeceptor on page 21](#)
- [FortiFirewall and FortiFirewallCarrier on page 21](#)
- [FortiMail on page 22](#)
- [FortiProxy on page 22](#)
- [FortiSandbox on page 22](#)
- [FortiSOAR on page 22](#)
- [FortiSwitch ATCA on page 23](#)
- [FortiTester on page 23](#)
- [FortiWeb on page 23](#)
- [Virtualization on page 23](#)



To confirm that a device model or firmware version is supported by the current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```



Always review the Release Notes of the supported platform firmware version before upgrading your device.

---

## Web browsers

FortiManager 7.0.6 supports the following web browsers:

- Microsoft Edge 102 (102.0.1245.33 or later)
- Mozilla Firefox version 101
- Google Chrome version 113



Please note the GUI may not work properly in Google Chrome version 114 (114.0.5735.91) and Microsoft Edge version 114 (114.0.1823.37).

---

Other web browsers may function correctly, but are not supported by Fortinet.

## FortiOS and FortiOS Carrier



The *FortiManager Release Notes* communicate support for FortiOS versions that are available at the time of the FortiManager 7.0.6 release. For additional information about other supported FortiOS versions, please refer to the FortiManager compatibility chart in the [Fortinet Document Library](#).

See [FortiManager compatibility with FortiOS](#).

---

FortiManager 7.0.6 supports the following versions of FortiOS and FortiOS Carrier:

- 7.0.0 to 7.0.11
- 6.4.0 to 6.4.12
- 6.2.0 to 6.2.14

## FortiADC

FortiManager 7.0.6 supports the following versions of FortiADC:

- 7.0.0 and later
- 6.2.0 and later
- 6.1.0 and later

## FortiAnalyzer

FortiManager 7.0.6 supports the following versions of FortiAnalyzer:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

## FortiAuthenticator

FortiManager 7.0.6 supports the following versions of FortiAuthenticator:

- 6.4.0 and later
- 6.3.0 and later
- 6.2.0 and later

## FortiCache

FortiManager 7.0.6 supports the following versions of FortiCache:

- 4.2.0 and later
- 4.1.0 and later
- 4.0.0 and later

## FortiClient

FortiManager 7.0.6 supports the following versions of FortiClient:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.1 and later

## FortiDDoS

FortiManager 7.0.6 supports the following versions of FortiDDoS:

- 6.3.0 and later
- 6.2.0 and later
- 6.1.0 and later

Limited support. For more information, see [Feature support on page 23](#).

## FortiDeceptor

FortiManager 7.0.6 supports the following versions of FortiDeceptor:

- 4.1 and later
- 4.0 and later
- 3.3 and later

## FortiFirewall and FortiFirewallCarrier

FortiManager 7.0.6 supports the following versions of FortiFirewall and FortiFirewallCarrier:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

## FortiMail

FortiManager 7.0.6 supports the following versions of FortiMail:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

## FortiProxy

FortiManager 7.0.6 supports configuration management for the following versions of FortiProxy:

- 7.0.7
- 7.0.6
- 7.0.5



Configuration management support is identified as *Management Features* in these release notes. See [Feature support on page 23](#).

---

FortiManager 7.0.6 supports logs from the following versions of FortiProxy:

- 7.0.0 to 7.0.7
- 2.0.0 to 2.0.5
- 1.2.0 to 1.2.13
- 1.1.0 to 1.1.6
- 1.0.0 to 1.0.7

## FortiSandbox

FortiManager 7.0.6 supports the following versions of FortiSandbox:

- 4.2.0 and later
- 4.0.0 and 4.0.1
- 3.2.0 and later
- 3.1.0 and later

## FortiSOAR

FortiManager 7.0.6 supports the following versions of FortiSOAR:

- 7.0.0 and later
- 6.4.0 and later

- 6.0.0 and later

## FortiSwitch ATCA

FortiManager 7.0.6 supports the following versions of FortiSwitch ATCA:

- 5.2.0 and later
- 5.0.0 and later
- 4.3.0 and later

## FortiTester

FortiManager 7.0.6 supports the following versions of FortiTester:

- 7.0.0 and later
- 4.2.0 and later
- 4.1.0 and later

## FortiWeb

FortiManager 7.0.6 supports the following versions of FortiWeb:

- 7.0.0 and later
- 6.4.0 and later
- 6.3.0 and later

## Virtualization

FortiManager 7.0.6 supports the following virtualization software:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Google Cloud Platform
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012, 2016, and 2019
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- Oracle Private Cloud
- VMware ESXi versions 6.5 and later

## Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiGate	✓	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓	✓
FortiADC		✓	✓		
FortiAnalyzer			✓	✓	✓
FortiAuthenticator					✓
FortiCache			✓	✓	✓
FortiClient		✓		✓	✓
FortiDDoS			✓	✓	✓
FortiDeceptor		✓			
FortiFirewall	✓				✓
FortiFirewall Carrier	✓				✓
FortiMail		✓	✓	✓	✓
FortiProxy	✓	✓	✓	✓	✓
FortiSandbox		✓	✓	✓	✓
FortiSOAR		✓	✓		
FortiSwitch ATCA	✓				
FortiTester		✓			
FortiWeb		✓	✓	✓	✓
Syslog					✓

## Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Japanese	✓	✓



Language	GUI	Reports
Korean	✓	✓
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings > Admin > Admin Settings*, in *Administrative Settings > Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiManager, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiManager. For more information, see the *FortiManager Administration Guide*.

## Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 7.0.6.



Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

This section contains the following topics:

- [FortiGate models on page 26](#)
- [FortiGate special branch models on page 28](#)
- [FortiCarrier models on page 32](#)
- [FortiCarrier special branch models on page 33](#)
- [FortiADC models on page 35](#)
- [FortiAnalyzer models on page 35](#)
- [FortiAuthenticator models on page 36](#)
- [FortiCache models on page 36](#)
- [FortiDDoS models on page 36](#)
- [FortiDeceptor models on page 37](#)
- [FortiFirewall models on page 37](#)
- [FortiFirewallCarrier models on page 37](#)
- [FortiMail models on page 38](#)
- [FortiProxy models on page 38](#)
- [FortiSandbox models on page 38](#)
- [FortiSOAR models on page 39](#)
- [FortiSwitch ATCA models on page 39](#)
- [FortiTester models on page 39](#)
- [FortiWeb models on page 40](#)

## FortiGate models

The following FortiGate models are released with FortiOS firmware. For information about supported FortiGate models on special branch releases of FortiOS firmware, see [FortiGate special branch models on page 28](#).

Model	Firmware Version
<b>FortiGate:</b> FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60EDSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F	7.0
<b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	
<b>FortiGate DC:</b> FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC	
<b>FortiGate ACDC:</b> FortiGate-2201E-ACDC, FortiGate-3960E-ACDC	
<b>FortiWiFi:</b> FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE	
<b>FortiGate VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen, FortiGate-VMX, FortiGate-VMX-Service-Manager, FortiGate-ARM64-AWS, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI,	
<b>FortiOS VM:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
<b>FortiGateRugged:</b> FortiGateRugged-60F, FortiGateRugged-60F-3G4G	

Model	Firmware Version
<b>FortiGate:</b> FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-80F-POE, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F	6.4
<b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	
<b>FortiGate DC:</b> FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC	
<b>FortiGate ACDC:</b> FortiGate-2201E-ACDC, FortiGate-3960E-ACDC	
<b>FortiGate Hardware Low Encryption:</b> FortiGate-100D-LENC	
<b>FortiWiFi:</b> FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F,	
<b>FortiGate VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen, FortiGate-VMX, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM	
<b>FortiOS VM:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
<b>FortiGateRugged:</b> FortiGateRugged-60F, FortiGateRugged-60F-3G4G	

Model	Firmware Version
<b>FortiGate:</b> FortiGate-30E, FortiGate-30E-3G4G-GBL, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FG-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FG-400E, FG-400E-Bypass, FG-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000C, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E <b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 <b>FortiGate DC:</b> FortiGate-80C-DC, FortiGate-401E-DC, FortiGate-600C-DC, FortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC <b>FortiGate Hardware Low Encryption:</b> FortiGate-80C-LENC, FortiGate-100D-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC <b>FortiWiFi:</b> FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-81F-2R-POE, <b>FortiGate-VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager <b>FortiOS:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen <b>FortiGate Rugged:</b> FortiGateRugged-30D, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-90D	6.2

## FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.0.6 supports these models on the identified FortiOS version and build number.

For information about supported FortiGate models released with FortiOS firmware, see [FortiGate models on page 26](#).

## FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-70F	7.0.8	4682
FortiGate-71F		
FortiGate-80F-DSL	7.0.10	4905
FortiGate-400F	7.0.10	4908
FortiGate-401F		
FortiGate-600F	7.0.10	4913
FortiGate-601F		
FortiGate-1000F	7.0.10	6503
FortiGate-1001F		
FortiGate-1500G	7.0.9	6458
FortiGate-1501G		
FortiGate-3000F	7.0.10	4908
FortiGate-3001F	7.0.10	4894
FortiGate-3200F	7.0.10	6506
FortiGate-3201F		
FortiGate-3700F	7.0.10	6506
FortiGate-3701F		
FortiGate-4800F	7.0.10	6506
FortiGate-4801F		
FortiGate-6000F	7.0.10	0117
FortiGate-6300F		
FortiGate-6300F-DC		
FortiGate-6301F		
FortiGate-6301F-DC		
FortiGate-6500F		
FortiGate-6500F-DC		
FortiGate-6501F		
FortiGate-6501F-DC		
FortiGate-7000E	7.0.10	0117
FortiGate-7030E		
FortiGate-7040E		
FortiGate-7060E		
FortiGate-7060E-8-DC		
FortiGate-7000F	7.0.10	0117
FortiGate-7121F		

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-7121F-2		
FortiGate-7121F-2-DC		
FortiGate-7121F-DC		
FortiGateRugged-70F	7.0.10	6509
FortiGateRugged-70F-3G4G	7.0.10	6524

## FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-400F	6.4.12	5429
FortiGate-401F		
FortiGate-600F	6.4.12	5429
FortiGate-601F		
FortiWiFi-80F-2R	6.4.8	5033
FortiWiFi-81F-2R		
FortiWiFi-81F-2R-3G4G-POE		
FortiWiFi-81F-2R-POE		
FortiWiFi-80F-2R-3G4G-DSL		
FortiGate-3500F	6.4.6	5886
FortiGate-3501F	6.4.6	6132
FortiGate-6000F	6.4.12	1914
FortiGate-6300F		
FortiGate-6300F-DC		
FortiGate-6301F		
FortiGate-6301F-DC		
FortiGate-6500F		
FortiGate-6500F-DC		
FortiGate-6501F		
FortiGate-6501F-DC		
FortiGate-7000E	6.4.12	1914
FortiGate-7030E		
FortiGate-7040E		
FortiGate-7060E		
FortiGate-7060E-8-DC		
FortiGate-7000F	6.4.12	1914
FortiGate-7121F		
FortiGate-7121F-2		

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-7121F-2-DC		
FortiGate-7121F-DC		

## FortiOS 6.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80D	6.2.13	5238
FortiGate-200F, FortiGate-201F	6.2.13	7249
FortiGate-1800F, FortiGate-1800F-DC FortiGate-1801F, FortiGate-1801F-DC	6.2.9	7197
FortiGate-2600F, FortiGate-2600F-DC FortiGate-2601F, FortiGate-2601F-DC	6.2.9	7197
FortiGate-4200F, FortiGate-4200F-DC FortiGate-4201F, FortiGate-4201F-DC	6.2.9	7197
FortiGate-4400F, FortiGate-4400F-DC	6.2.9	7197
FortiGate-4401F, FortiGate-4401F-DC	6.2.9	7197
FortiGate-6000F FortiGate-6300F FortiGate-6300F-DC FortiGate-6301F FortiGate-6301F-DC FortiGate-6500F FortiGate-6500F-DC FortiGate-6501F FortiGate-6501F-DC	6.2.13	1271
FortiGate-7000E FortiGate-7030E FortiGate-7040E FortiGate-7060E FortiGate-7060E-8-DC	6.2.13	1271
FortiGate-7000F FortiGate-7121F FortiGate-7121F-2 FortiGate-7121F-2-DC FortiGate-7121F-DC	6.2.13	1271
FortiWiFi-80F-2R-3G4G-DSL FortiWiFi-81F-2R-3G4G-DSL	6.2.6	7219

FortiGate Model	FortiOS Version	FortiOS Build
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099

## FortiCarrier models

Model	Firmware Version
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4400F-DC, FortiCarrier-4400F-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen, FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI	7.0
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4400F-DC, FortiCarrier-4400F-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1	6.2



Model	Firmware Version
<b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC	
<b>FortiCarrier 6K and 7K:</b> FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7000F, FortiCarrier-7121F, FortiCarrier-7121F-2	
<b>FortiCarrier 6K and 7K DC:</b> FortiCarrier-6000F-DC, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC, FortiCarrier-7060E-8-DC, FortiCarrier-7121F-DC, FortiCarrier-7121F-2-DC	
<b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALL, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	

## FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 7.0.6 supports these models on the identified FortiOS Carrier version and build number.

For information about supported FortiCarrier models released with FortiOS Carrier firmware, see [FortiCarrier models on page 32](#).

### FortiCarrier 7.0

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3000F	7.0.10	4908
FortiCarrier-3001F	7.0.10	4894
FortiCarrier-3200F FortiCarrier-3201F	7.0.10	6506
FortiCarrier-3700F FortiCarrier-3701F	7.0.10	6506
FortiCarrier-4800F FortiCarrier-4801F	7.0.10	6506
FortiCarrier-6000F FortiCarrier-6300F FortiCarrier-6300F-DC FortiCarrier-6301F FortiCarrier-6301F-DC FortiCarrier-6500F FortiCarrier-6500F-DC	7.0.10	0117

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-65001F		
FortiCarrier-6501F-DC		
FortiCarrier-7000E	7.0.10	0117
FortiCarrier-7030E		
FortiCarrier-7040E		
FortiCarrier-7060E		
FortiCarrier-7060E-8-DC		
FortiCarrier-7000F	7.0.10	0117
FortiCarrier-7081F		
FortiCarrier-7121F		
FortiCarrier-7121F-DC		
FortiCarrier-7121F-2		
FortiCarrier-7121F-2-DC		

## FortiCarrier 6.4

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3500F	6.4.6	5886
FortiCarrier-3501F	6.4.6	6132
FortiCarrier-6000F	6.4.12	1914
FortiCarrier-6300F		
FortiCarrier-6300F-DC		
FortiCarrier-6301F		
FortiCarrier-6301F-DC		
FortiCarrier-6500F		
FortiCarrier-6500F-DC		
FortiCarrier-65001F		
FortiCarrier-6501F-DC		
FortiCarrier-7000E	6.4.12	1914
FortiCarrier-7030E		
FortiCarrier-7040E		
FortiCarrier-7060E		
FortiCarrier-7060E-8-DC		
FortiCarrier-7000F	6.4.12	1914
FortiCarrier-7081F		
FortiCarrier-7121F		
FortiCarrier-7121F-DC		
FortiCarrier-7121F-2		

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-7121F-2-DC		

## FortiADC models

Model	Firmware Version
<b>FortiADC:</b> FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F <b>FortiADC VM:</b> FortiADC-VM	6.2, 7.0
<b>FortiADC:</b> FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F <b>FortiADC VM:</b> FortiADC-VM	6.0, 6.1

## FortiAnalyzer models

Model	Firmware Version
<b>FortiAnalyzer:</b> FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E <b>FortiAnalyzer VM:</b> FortiAnalyzer-DOCKER, FortiAnalyzer-VM64, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.0
<b>FortiAnalyzer:</b> FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E <b>FortiAnalyzer VM:</b> FortiAnalyzer-DOCKER, FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	6.4

Model	Firmware Version
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-200F, FAZ-300D, FAZ-300F, FAZ-300G, FAZ-400E, FAZ-800F, FAZ-1000D, FAZ-1000E, FAZ-1000F, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3000G, FAZ-3500E, FAZ-3500F, FAZ-3500G, FAZ-3700F and FAZ-3900E.	6.2
<b>FortiAnalyzer VM:</b> FortiAnalyzer-DOCKED, FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	

## FortiAuthenticator models

Model	Firmware Version
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E	6.2, 6.3, 6.4
<b>FortiAuthenticator VM:</b> FAC-VM	

## FortiCache models

Model	Firmware Version
<b>FortiCache:</b> FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E	4.1, 4.2
<b>FortiCache VM:</b> FCH-KVM, FCH-VM64	
<b>FortiCache:</b> FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E	4.0
<b>FortiCache VM:</b> FCH-VM64	

## FortiDDoS models

Model	Firmware Version
<b>FortiDDoS:</b> FortiDDoS-2000F	6.3
<b>FortiDDoS:</b> FortiDDoS-200F, FortiDDoS-1500F	6.1, 6.2, 6.3
<b>FortiDDoS VM:</b> FortiDDoS-VM	

## FortiDeceptor models

Model	Firmware Version
<b>FortiDeceptor:</b> FDC-1000F, FDC-1000G <b>FortiDeceptor Rugged:</b> FDCR-100G <b>FortiDeceptor VM:</b> FDC-VM	4.1
<b>FortiDeceptor:</b> FDC-1000F, FDC-1000G <b>FortiDeceptor Rugged:</b> FDCR-100G <b>FortiDeceptor VM:</b> FDC-VM	4.0
<b>FortiDeceptor:</b> FDC-1000F, FDC-3000D <b>FortiDeceptor VM:</b> FDC-VM	3.3

## FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.0.6 supports these models on the identified FortiFirewall firmware version and build number.

Model	Firmware Version	Firmware Build
<b>FortiFirewall:</b> FortiFirewall-3980E, FortiFirewall-4200F, FortiFirewall-4400F <b>FortiFirewall DC:</b> FortiFirewall-3980E-DC <b>FortiFirewall VM:</b> FortiFirewall-VM64, FortiFirewall-VM64-KVM	6.4	1999
<b>FortiFirewall:</b> FortiFirewall-4401F <b>FortiFirewall DC:</b> FortiFirewall-4401F-DC	6.4	5423
<b>FortiFirewall:</b> FortiFirewall-2600F <b>FortiFirewall DC:</b> FortiFirewall-2600F-DC	6.4	5423
<b>FortiFirewall:</b> FortiFirewall-1801F <b>FortiFirewall DC:</b> FortiFirewall-1801F-DC	6.4	5423
<b>FortiFirewall:</b> FortiFirewall-3980E <b>FortiFirewall DC:</b> FortiFirewall-3980E-DC	6.2	1262
<b>FortiFirewall:</b> FortiFirewall-4200F	6.2.7	5141
<b>FortiFirewall:</b> FortiFirewall-4400F	6.2.7	5148

## FortiFirewallCarrier models

The following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.0.6 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version	Firmware Build
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.4	1999
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4401F	6.4	5423
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.2.7	5148

## FortiMail models

Model	Firmware Version
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E <b>FortiMail VM:</b> FML-VM	7.0
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E <b>FortiMail VM:</b> FML-VM	6.2, 6.4

## FortiProxy models

Model	Firmware Version
<b>FortiProxy:</b> FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G <b>FortiProxy VM:</b> FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.0
<b>FortiProxy:</b> FPX-400E, FPX-2000E, FPX-4000E <b>FortiProxy VM:</b> FortiProxy-KVM, FortiProxy-VM64	1.2, 2.0

## FortiSandbox models

Model	Firmware Version
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D <b>FortiSandbox DC:</b> FSA-1000F-DC <b>FortiSandbox-VM:</b> FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	4.0, 4.2
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox DC:</b> FSA-1000F-DC <b>FortiSandbox-VM:</b> FortiSandbox-AWS, FSA-VM	3.1, 3.2

## FortiSOAR models

Model	Firmware Version
<b>FortiSOAR VM:</b> FortiSOAR-VM	6.0, 6.4, 7.0

## FortiSwitch ATCA models

Model	Firmware Version
<b>FortiController:</b> FTCL-5103B, FTCL-5903C, FTCL-5913C	5.2
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B <b>FortiController:</b> FTCL-5103B	5.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B	4.3

## FortiTester models

Model	Firmware Version
<b>FortiTester:</b> FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F <b>FortiTester VM:</b> FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.0
<b>FortiTester:</b> FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F <b>FortiTester VM:</b> FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	4.2
<b>FortiTester:</b> FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F <b>FortiTester VM:</b> FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	4.1

## FortiWeb models

Model	Firmware Version
<b>FortiWeb:</b> FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-2000F, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3000F, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E, FortiWeb-4000F <b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.4, 7.0
<b>FortiWeb:</b> FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E <b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.3



# Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 7.0.6. Compatibility issues have been identified for the following FortiOS releases:

FortiOS 7.0

- [FortiManager 7.0.6 and FortiOS 7.0.11 compatibility issues on page 41](#)

## FortiManager 7.0.6 and FortiOS 7.0.11 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.0.6 and FortiOS 7.0.11. FortiOS 7.0.11 includes syntax changes not supported by FortiManager 7.0.6.



When specific platforms are indicated, the syntax change applies to both the FortiGate and FortiCarrier platform for the model.

For example, (4 platforms: 3980E,3960E) indicates FortiGate-3980E, FortiCarrier-3980E, FortiGate-3960E, FortiCarrier-3960E.

The following objects were added:

- (attr) endpoint-control fctems ca-cn-info
- (attr) endpoint-control fctems trust-ca-cn
- (node) system replacemsg custom-message

The following default values changed:

- system interface mediatype default value changed from none to qsfp28-sr4
- system lte-modem auto-connect default value changed from disable to enable
- system lte-modem gps-service default value changed from disable to enable
- system npu hash-config default value is changed depending on the platform. For more information, see the [FortiOS Hardware Acceleration Guide](#) on the Fortinet Documents Library.

Additional option changes:

```
system interface mediatype
  option-list (tag|opt): ["cr", "cr4", "gmii", "lr", "lr4", "none", "sgmii", "sr",
    "sr4"] -> None (4 platforms: 3980E,3960E)
  option-list (tag|opt): None -> ["qsfp28-cr4", "qsfp28-lr4", "qsfp28-sr4"] (4
    platforms: 3980E,3960E)
system interface speed
  option-list (tag|opt): None -> ["2500auto", "5000auto"] (36 platforms:
    2200E,3301E,3980E,2601F,3501F,4200F,3500F,1800F,3600E,1100E,4401F,2201E,1801F,330
    0E,3400E,2600F,4201F,3601E,1101E,3960E,3401E,4400F)
system link-monitor interval
  int-range (tag|lmt): 500,3600000 -> 20,3600000
system link-monitor probe-timeout
  int-range (tag|lmt): 500,5000 -> 20,200
system sdwan health-check interval
  int-range (tag|lmt): 500,3600000 -> 20,3600000
```

```
system sdwan health-check probe-timeout
  int-range (tag|lmt): 500,3600000 -> 20,3600000
webfilter profile
  tab-size (tag|tz): 20000,20000,0 -> 35000,35000,0 (16 platforms:
    4200F,4401F,4201F,3601E,3980E,3600E,3960E,4400F)
webfilter urlfilter
  tab-size (tag|tz): 1000,1000,0 -> 35000,35000,0 (16 platforms:
    4200F,4401F,4201F,3601E,3980E,3600E,3960E,4400F)
```

# Resolved Issues

The following issues have been fixed in 7.0.6. To inquire about a particular bug, please contact [Customer Service & Support](#).

## AP Manager

Bug ID	Description
853345	The clients are connected to the Wireless Access Point; however, "clients" section under the diagnostics & tools of AP does not display any info.

## Device Manager

Bug ID	Description
845656	When BGP is enabled and no IP address is defined for <code>set-ip-nexthop</code> under the route-map config, FortiManager tries to set the IP to 0.0.0.0, and this may break the BGP network.
853061	Installation fails as FortiManager attempts configuring "allowas-in6" on neighbor when configuring router bgp via BGP template.
855425	<i>System Template</i> and <i>CLI Template</i> config did not install to all model device FortiGates.
856207	FortiGate's WAN1 interface cannot be edited via FortiManager's GUI.
859249	After upgrade, <i>Firmware Templates</i> under the <i>Device Manager</i> is blank. Even new entries cannot be created.
874811	FortiManager tries to set the "set-ip-nexthop" to "0.0.0.0" during the installation.

## Others

Bug ID	Description
838638	FortiGates are upgraded successfully via FortiManager's Group Firmware upgrade feature; however, the task monitor displays "Image upgrade failed" for some of the FortiGates.
845753	IPSec installation fails on Google Cloud Platform (GCP) ONDEMAND FortiGate.
850467	Unprivileged Users might be able to disclose unauthorized information via API.

Bug ID	Description
851354	Installation while using CLI templates may fail and create the "securityconsole" Application crash.
855840	'allowaccess' on interfaces completely removed on GCP ONDEMAND FortiGate.

## Policy and Objects

Bug ID	Description
827602	Unable to import EMS Tags from EMS Server.
827607	The enable/disable status feature for the EMS Connector is not available on FortiManager.
841492	FortiManager unsets the system HA settings after pushing an unsuccessful installation Policy Package to FortiGates.
850105	Unable to perform Apply & Refresh on EMS Connector.
853347	ZTNA tags name/format from EMS/FortiGates don't match with the ones from FortiManager's DB.
866724	Copy Failed error has been observed with the error message, "Virtual server limit reached!"; this limit is 50 for FGT AWS ONDEMAND.
868937	GUI VIP Mapped IPv6 Address/Range gives "Mapping to IP 0 not allowed".
873896	Unable to remove "(null)" objects under "endpoint-control".
874188	Installation fails due to FortiManager's attempts to remove the "endpoint-control fctems" entries.
875980	FortiManager unsets EMS connector Serial Number and the tenant-id during the installation.

## System Settings

Bug ID	Description
848934	SNMPv3 does not work properly on FortiManager and FortiAnalyzer.

## VPN Manager

Bug ID	Description
798995	It's not possible to delete an SSL VPN portal profile from FortiManager GUI if the profile has been already installed.

## Common Vulnerabilities and Exposures

Visit <https://fortiguard.com/psirt> for more information.

Bug ID	CVE references
872711	FortiManager 7.0.6 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2023-22642</li></ul>

# Known Issues

The following issues have been identified in 7.0.6. To inquire about a particular bug or to report a bug, please contact [Customer Service & Support](#).

## AP Manager

Bug ID	Description
822525	FortiManager does not take the per device mapping authentication config for SSID under the Wifi Profiles.
824032	Some of the FAPs Radio configuration settings under the AP's profile are missing.

## Device Manager

Bug ID	Description
752443	Vertical scroll bar is missing in SD-WAN configuration.
789249	FortiManager does not have Logging Options after enabling One-Arm Sniffer under Interface.
789544	Status of the "Firmware Template" has been changed to "Unknown" after upgrade.
794764	FortiGate Modem Interface is not visible under <i>Device Manager</i> .
800191	During the ZTP deployment, "set hostname" command does not push to FortiGate.
801547	When removing an entry in the static route template, static route entries are shifted and the installation fails.
807771	FortiManager unsets the gateway settings in SDWAN template after upgrading ADOM from v6.4 to v7.0.
810936	After Upgrade, managed FortiAnalyzer on FortiManager does not display the Traffic logs under the <i>Log View</i> for HA devices.
815901	The router static entries created by IPSEC template are deleted and re-created after upgrade.
817346	Editing interface with normalized interface mapping displays some unnecessary messages for mapping change.
818905	FortiManager unsets the certificate for "endpoint-control fctems" setting during the installation.
828897	<i>SD-WAN Monitor</i> map doesn't load all devices.

Bug ID	Description
829404	SD-WAN Widget does not display any data for "Bandwidth Overview" and "Traffic Growth" under the Managed Devices' dashboard.
835106	FortiManager cannot sync its devices with FortiAnalyzer when adding it to the <i>Device Manager</i> ; it displays the error message "Serial number already in use".
837213	Browser may crash when clicking "view diff" to compare with current device config. This might happen due to the network slowness. <b>Workaround:</b> Use "show diff only" from Revision History instead of checking it from "Out of Sync" devices list."
839334	FortiManager does not allow empty value for "Interface Preference" as SD-WAN Rules under the SD-WAN Templates.
850471	FortiManager is attempting to modify replacement messages after upgrade, which leads to installation failure.
853810	Failed to edit the managed devices to modify the location.
855032	FortiManager displays the total devices/VDOMs count incorrectly when split VDOM enabled on FortiGates.
859638 860071	FortiManager's SD-WAN monitor does not display the Health Check status correctly.
861220	Leaving the SD-WAN member empty when configuring the SD-WAN using the template fails due to the syntax differences between FortiGate and FortiManager.
861238	<i>SD-WAN Monitor</i> , under <i>Device Manager's</i> Monitors, displays an Unknown status (a grey question mark) icon for HA devices under the Map View.
866243	The <i>SD-WAN Monitor</i> info for specific devices are not consistent with the map view SD-WAN interface status (based on performance SLA).
866247	Unable to change the static route "Description" section in the <i>Device Manager</i> without editing the static route.
870848	<i>SD-WAN Monitor</i> under <i>Device Manager's</i> Monitors tab does not display any FortiGate devices which are running in 6.2 version.
872865	FortiManager attempts to set a default value like "system cluster-sync" on FortiGate, and this causes installation failure.
874831	FortiManager attempts to install unknown and undesired static route when modifying or adding some new static routes.

## FortiSwitch Manager

Bug ID	Description
818842	FortiManager displays "Failed loading data" for "Security Policy", "LLDP Profile", and "QoS

Bug ID	Description
	Policy" features when editing ports in Per-device mode FortiSwitch Management.
868949	Installation fails as <i>FortiSwitch Manager</i> creates an alias name longer than the total limit 25 characters.
872802	FortiManager automatically sets "default" as <code>dnsfilter-profile</code> under <code>dns-server</code> for <code>fortilink</code> interface.

## Global ADOM

Bug ID	Description
826522	Unable to remove global object from Global Database in workspace mode. <b>Workaround:</b> Unlock & lock the Global ADOM prior to deleting the Global Object and assigning changes to local ADOMs.
868212	Assigning global policies to ADOMs by admins with access to specific ADOMs fails.
870944	Global Policy Assignment displays the following error (Double global assignment exists).

## Others

Bug ID	Description
713714	The schedule for firmware upgrade for FortiGates does not work if the upgrade request is issued from the CLI; instead, firmware upgrade starts immediately. <b>Workaround:</b> Use firmware upgrade templates in the GUI.
745958	Unable to config ipsec tunnel using the ipsec tunnel template.
777028	FortiManager does not support the FortiCarrier-7121F.
777831	When FortiAnalyzer is added as a managed device to FortiManager, the "Incident & Event" tile will be displayed instead of the "FortiSoC" tile.
814425	Sorting FortiExtenders by Network, RSSI, RSRP, RSRQ, and SINR does not work properly.
816936	FortiManager does not support the FGT/FGC 7KE/7KF syntax.
820921	FortiManager displays incorrect device firmware versions for FortiSandbox and FortiMail.
822263	Service Status under FortiGuard does not display the secondary Service status of the FortiGate's cluster correctly.
832351	FortiManager does not allow users to enter to the root ADOM; it displays the "ADOM license was expired..." message.
839586	FortiManager does not save applying the configuration of "Enable AntiVirus and IPS service



Bug ID	Description
	for FortiDeceptor" under FortiGuard settings pane.
850377	In Workflow Mode, when new session is created, the Policies disappear.
857659	FortiManager did not download the "AI Malware Engine" Package from FortiGuard Server.
865200	Users encountered unsatisfactory performance of FortiManager due to several crashes on the "Application fmgd" process.
870893	Unable to install pp to FortiGates after FortiManager's DB got restored.
871608	Unable to retrieve routing information from FortiGate via FortiManager when there is a large routing table.
874369	Upgrading FortiManager fails due to some invalid data for managed FortiExtender's Objects.
876425	FortiManager does not display the output of the "execute dmserver showconfig".
891869	FortiManager wrongly recommends lower version for upgrade the FortiGates.
919088	GUI may not work properly in Google Chrome and Microsoft Edge version 114.

## Policy & Objects

Bug ID	Description
585177	FortiManager is unable to create VIPv6 virtual server objects.
698838	"Download Conflict File" does not display all of the firewall objects conflicts when importing policy packages from FortiGate to FortiManager.
738988	FortiManager does not detect the settings related to Web Cache Communication Protocol (WCCP) in SSLVPN Policies on the FortiGate.
741269	Unable to install configuration to FortiGates due to the error message "Resource temporarily unavailable".
751443	<p>FortiManager displays policy installation copy failures error when ipsec template gets unassigned.</p> <p><b>Workaround:</b> Instead of unassigning IPSec template, modify IPSec template, replace the reference to IPSec tunnel interface with another interface. Please ensure a fresh FortiManager backup is created prior to any changes.</p>
752993	VPN IPSEC installation fails as phase1 settings on FortiManager are not consistent with the ones on FortiOS.
774058	Rule list order may not be saved under File Filter Profile.
793240	<p>FortiManager fails to retrieve FortiGate's configuration when external-resource objects include a "g-" prefix.</p> <p>There are two workarounds; use the approach that works best for your environment. If it is possible, create a new backup of your FMG and FGT(s) before making any changes:</p>

Bug ID	Description
	<p>First workaround approach:</p> <ol style="list-style-type: none"> <li>1. Re-create all threat feeds locally in VDOM configuration and update policies and security profiles that reference them to the local threat feed vs. the global feed.</li> <li>2. Delete the global threat feed objects.</li> </ol> <p>Second workaround approach:</p> <ol style="list-style-type: none"> <li>1. Perform policy reinstallation. FMG adds original threat feed objects within the VDOM configuration without the 'g' prefix.</li> <li>2. FMG reports 'install OK/verify FAIL' at the end of the policy installation.</li> <li>3. Run scripts to delete the global threat feed objects (objects with the 'g' prefix) from the FGT.</li> <li>4. Retrieve the FGT configuration from FMG.</li> <li>5. Perform another policy installation to update the configuration synchronization status between the FGT and FMG. No commands are pushed during this stage according to the install wizard.</li> </ol>
795449	Unable to "Download Conflict File" to review the conflicts of firewall objects during import process.
803460	"User Definitions" entries under the "User & Authentication" cannot be removed from FortiManager.
810073	Fail to import the firewall policy due to the "interface mapping undefined" error message.
814364	FortiManager does not support the FCT EMS prefix; therefore, policies with ZTNA Tags cannot be installed properly to the FortiGates.
817220	FortiManager does not support the "userPrincipalName" as the common Name Identifier for LDAP Server configuration.
819847	FortiManager displays a false warning message "Duplicate Objects With Same Values" when creating the Firewall Objects' Service entries under the <i>Policy &amp; Objects</i> .
824652	Under the "Advanced Options" for firewall policy, "session-ttl" feature cannot be set to "never".
827416	FortiManager does not display any copy failure errors when utilized objects do not have any default values or per-device mapping.
834806	Installation fails due to extra back slashes when installing the custom IPS signatures to the FortiGates.
835087	Policies cannot be edited as FortiManager displays a warning message, "Please select a SSL/SSH Inspection profile" in ADOM 6.2.
845022	SDN Connector failed to import objects from VMWare VSphere.
846634	GUI does not allow to edit the custom Application and Filter Overrides
847932	Hit count for a policy package does not always match the total count of all installation targets.
848666	"Install Device" task stuck without any progress when installing the templates and firewall policies to the FortiGates.

Bug ID	Description
858183	After firmware's upgrade, virtual wire pair interfaces are missing in virtual wire pair interface policy.
859217	Rearranging the Destination NAT (DNAT) objects whose names contain special characters displays an error message "object does not exist".
862014 880359	FortiManager is purging 'replacement message group custom' configuration after install verification fails.
862727	Policy Package installation failed due to the error "native vlan must be set" message.
862839	Cloning the Policy Packages on FortiManager creates the duplicate UUIDs.
863882	'Last Modified Time' field is empty when exporting Policy Packages to Excel.
867809	During installation, FortiManager unsets status for the proxy policies.
870688	Editing the "Install On" changes the Policy status to "Modified" for all FortiGates existing on that rule.
875547	Policy & Package cannot be imported if the type of firewall address in FortiGate is "interface-subnet" and subnet's value is different with its value on FortiManager.
881857	Multiple security console Application crashes have been observed during the Policy Package installation when static router template and router static entry in device db are used.
882996	Unable to install to FortiGates when using null values for "local-gw6" and "remote-gw6".
886911	FortiManager is attempting to modify replacement messages after upgrade, and this leads to installation failure.
889563	FortiManager, for ADOM version 6.4, does not support Creating, Importing, or Inserting Above and Below actions for a deny policy with a "Log Violation Traffic" disabled. <b>Workarounds:</b> <ul style="list-style-type: none"> <li>To Insert, use copy &amp; paste instead of the using Insert Above/Below.</li> <li>To Create, either run script to create log disabled deny policy or enable log traffic first, and then edit the policy in order to disable and save it.</li> </ul>
891106	ZTNA Tags cannot be downloaded by EMS Cloud connector.

## Revision History

Bug ID	Description
801614	FortiManager might display an error message "Failed to create a new revision." for some FortiGates, when retrieving their configurations.

## System Settings

Bug ID	Description
753204	Admins of a specific ADOM are able to see tasks of others ADOMs.
825319	FortiManager fails to promote a FortiGate HA member (running on firmware 7.2.0 to 7.2.4) to the Primary.
850469	Radius group attribute filter does not work with Microsoft NFS.
851029	FortiManager's HA cluster breaks after upgrading the FortiManager.
853353	SDWAN Monitor Map does not show up when admin profile has been set to "None" for System Settings.
862814	Event logs did not log FortiManager admins and their actions on managed devices.
864041	SNMPv3 stopped working after upgrading the FortiManager.
864420	The presence of the default system admin information in the "sysconfdef" directory files may pose a potential security risk. Hence, it is advised to remove this potential security concern from these def files.
864931	Unable to login into FortiManager using TACACS and Radius credentials.
868706	SSO admin users do not have the same permissions as local users with the same assigned profiles.
873078	FortiManager HA cannot be configured as the initial sync never completes.

## VPN Manager

Bug ID	Description
762401	FortiManager is unable to preserve the Specify custom IP ranges option for SSL VPN Address range setting.
784385	<p>If policy changes are made directly on the FortiGates, the subsequent PP import creates faulty dynamic mappings for <i>VPN Manager</i>.</p> <p><b>Workaround:</b></p> <p>It is strongly recommended to create a fresh backup of the FortiManager's configuration prior to this workaround. Perform the following command to check &amp; repair the FortiManager's configuration database:</p> <pre>diagnose cdb check policy-packages &lt;adom&gt;</pre> <p>After running this command, FortiManager will remove the invalid mappings of vpnmgr interfaces.</p>

## Appendix A - FortiGuard Distribution Servers (FDS)

In order for FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as an FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the following items:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default, and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through port 443.

### FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform:

Platform	Update Service	Query Service
FortiGate	✓	✓
FortiADC	✓	
FortiCache	✓	
FortiCarrier	✓	✓
FortiClient	✓	
FortiDeceptor	✓	✓
FortiDDoS	✓	
FortiEMS	✓	
FortiMail	✓	✓
FortiProxy	✓	✓
FortiSandbox	✓	✓
FortiSOAR	✓	
FortiTester	✓	
FortiWeb	✓	

## Appendix B - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiManager hardware models and virtual machines.

### Hardware models

FortiManager supports a default number of ADOMs based on hardware model.

Some hardware models support an ADOM subscription license. When you purchase an ADOM subscription license, you increase the number of supported ADOMs. For example, you can purchase an ADOM subscription license for the FMG-3000G series, which allows you to use up to a maximum of 8000 ADOMs.

Other hardware models do not support the ADOM subscription license. For hardware models that do not support the ADOM subscription license, the default and maximum number of ADOMs is the same.

FortiManager Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
200G Series	30		30
300F Series	100		100
400G Series	150		150
1000F Series	1000		1000
2000E Series	1200		1200
3000G Series	4000	✓	8000
3700G Series	10,000	✓	12,000

For FortiManager F series and earlier, the maximum number of ADOMs is equal to the maximum devices/VDOMs as described in the [FortiManager Data Sheet](#).

### Virtual Machines

FortiManager VM subscription license includes five (5) ADOMs. Additional ADOMs can be purchased with an ADOM subscription license.

For FortiManager VM perpetual license, the maximum number of ADOMs is equal to the maximum number of Devices/VDOMs listed in the [FortiManager Data Sheet](#).



FortiManager VM subscription and perpetual licenses are stackable.

---



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.